Apache Log4cxx, Apache Log4cxx (Conan), Apache Log4cxx (Brew): Silent log event loss in XMLLayout due to unescaped XML 1.0 forbidden characters

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40023
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 16:16:32 UTC
Updated	2026-04-10 17:17:12 UTC
Description	Apache Log4cxx's XMLLayout https://logging.apache.org/log4cxx/1.7.0/classlog4cxx_1_1xml_1_1XMLLayout.html , in vers

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from security@apache.org

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-116 | CWE-116 CWE-116 Improper Encoding or Escaping of Output

Version	Source	Type	Score	Severity	Vector
4.0	security@apache.org	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Log4cxx	affected 1.7.0 semver	Not specified
CNA	Apache Software Foundation	Apache Log4cxx Conan	affected 1.7.0 semver	Not specified
CNA	Apache Software Foundation	Apache Log4cxx Brew	affected 1.7.0 semver	Not specified

References

Reference	Source	Link
logging.apache.org/log4cxx/1.7.0/classlog4cxx_1_1xml_1_1XMLLayout.html	security@apache.org	logging.apache.o
logging.apache.org/cyclonedx/vdr.xml	security@apache.org	logging.apache.o
logging.apache.org/security.html	security@apache.org	logging.apache.o
lists.apache.org/thread/y15cv3zblg3dfwr5vy6ddbnl4zyrzr8b	security@apache.org	lists.apache.org
www.openwall.com/lists/oss-security/2026/04/10/12	af854a3a-2127-422b-91ae-364da2661108	www.openwall.co
github.com/apache/logging-log4cxx/pull/609	security@apache.org	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Olawale Titiloye (en)

Additional Advisory Data

Source	Time	Event

CNA	2026-03-15T06:05:00.000Z	Vulnerability reported by Olawale Titiloye
CNA	2026-03-16T06:31:00.000Z	Fix shared publicly by Stephen Webb as pull request #609
CNA	2026-04-04T03:14:00.000Z	Log4cxx 1.7.0 released

There are currently no legacy QID mappings associated with this CVE.